Cybersecurity Incident Report:
SYN Flood Network Attack

Part 1: Identify the problem

The likely attack identified is: A TCP SYN flood attack, which is a form of Denial of Service (DoS).

Summary of the packet capture analysis:
• Numerous TCP SYN requests were observed from IP address 203.0.113.0 targeting the web server (192.0.2.1) on port 443.
• The requests never completed the three-way handshake (no ACKs), leaving the server with half-open connections.
• This behavior is consistent with a SYN flood attack.

Relevant tcpdump Log Excerpts:

No.	Time	Source	Destination	Protocol	Info
5	52	3.390692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN]
10	57	3.664863	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN]
14	61	3.939499	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN]
23	70	5.237887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN]
30	77	7.330577	192.0.2.1	198.51.100.5	HTTP	504 Gateway Time-out
37	84	7.581629	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN]
55	102	17.005862	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN]
103	150	29.212108	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN]
149	196	44.070706	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN]
167	212	49.238914	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN]

Part 2: Analysis and Impact

Description of the attack: The web server was targeted by a SYN flood, where an attacker sent a continuous stream of SYN packets without completing the handshake. This left the server with a large number of half-open connections, exhausting its resources.

How it affected the organization:
• The web server became overloaded and unresponsive.
• Employees could not access the internal sales webpage.
• Customers experienced timeout errors when trying to load the company’s website.

Consequences of the attack:
• Business disruption due to loss of productivity.
• Potential revenue loss from customers unable to access promotions or make purchases.
• Reputational damage due to website downtime.

Immediate actions taken: The server was temporarily taken offline to recover, and firewall rules were applied to block traffic from the malicious IP address (203.0.113.0).

Limitations of this response: Blocking a single IP address is insufficient, as attackers can spoof or rotate addresses.

Recommended next steps:
• Implement SYN cookies to mitigate half-open connection exhaustion.
• Deploy IDS/IPS solutions to detect and block SYN flood traffic.
• Use upstream DDoS protection (cloud WAF, traffic scrubbing).
• Apply load balancing and rate-limiting to reduce impact on a single server.